RSAC 2025 Conference

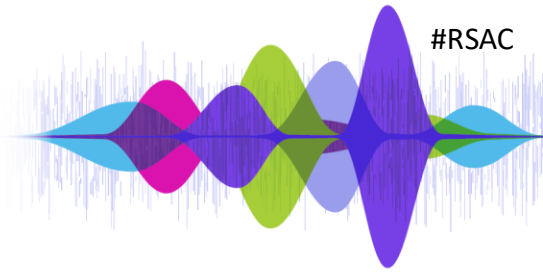
Many Voices.
One Community.

SESSION ID: CSO-T02

A Deep Dive into the New SEC Cybersecurity Disclosure Requirements

Jeff Pollard

Vice President, Principal Analyst
Forrester
https://www.linkedin.com/in/jpollard96/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Whenever there's – yet another – new regulation

By the end of this you'll feel better I promise

What You'll Learn Today

- The details of the SEC disclosure requirements
- The common organizational structure, controls, and frameworks publicly traded firms use to satisfy these requirements
- How to comply by weaponizing ambiguity

RSAC 2025 Conference

What We Learned In Our Deep Dive

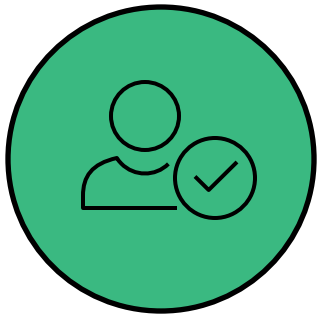
Three big takeaways in this research

Clouds the push for transparency

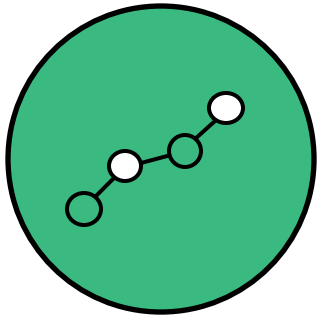
The definition of materiality is the topic du jour

Credentials and competence to evangelize security leaders

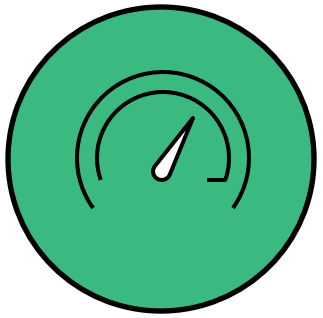
Guesswork clouds the push for transparency



Still unclear exactly what the SEC wants in each section



Questionable link to risk tolerance, appetite, or security posture



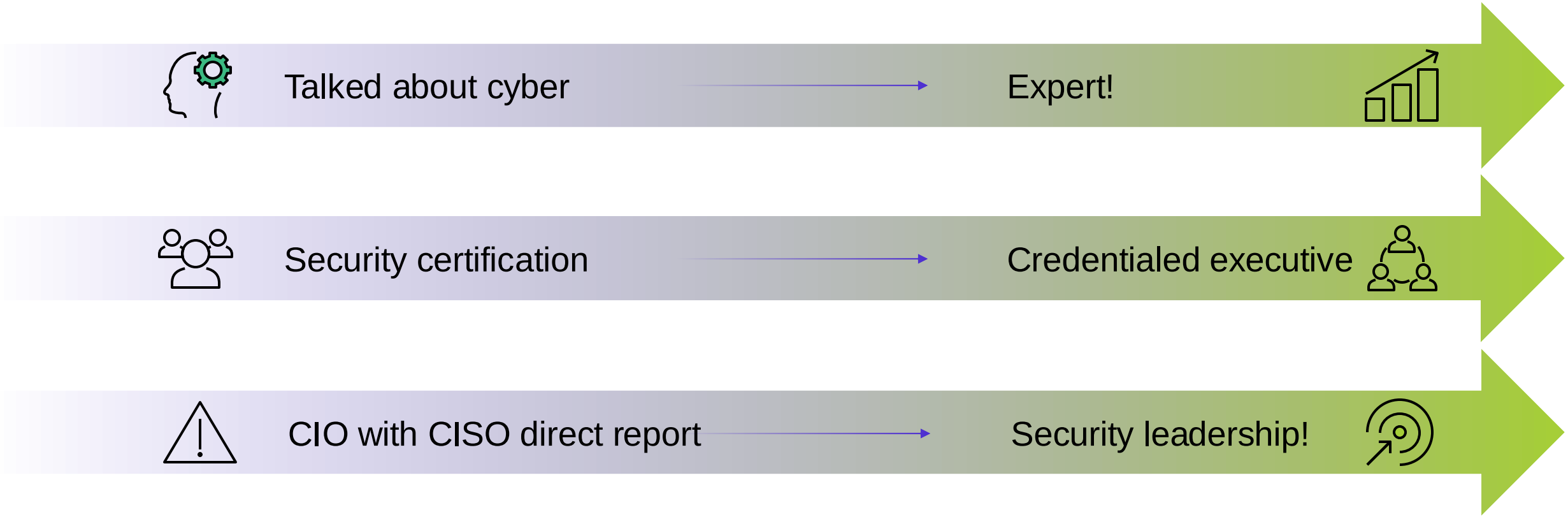
Difference between “cyber governance” and corporate governance

Exploiting The Definition Of Materiality

"A matter is material if there is a substantial likelihood that a reasonable investor would consider it important when determining whether to buy or sell securities."

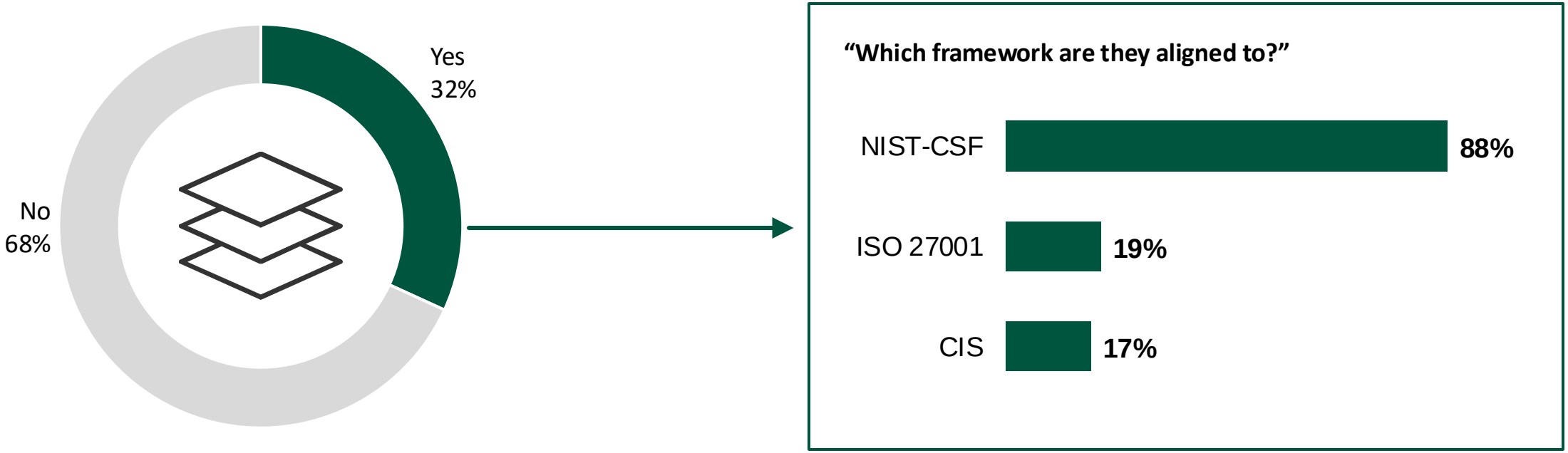
— U.S. Securities and Exchange Commission (SEC)

Credential inflation is back and better than ever!



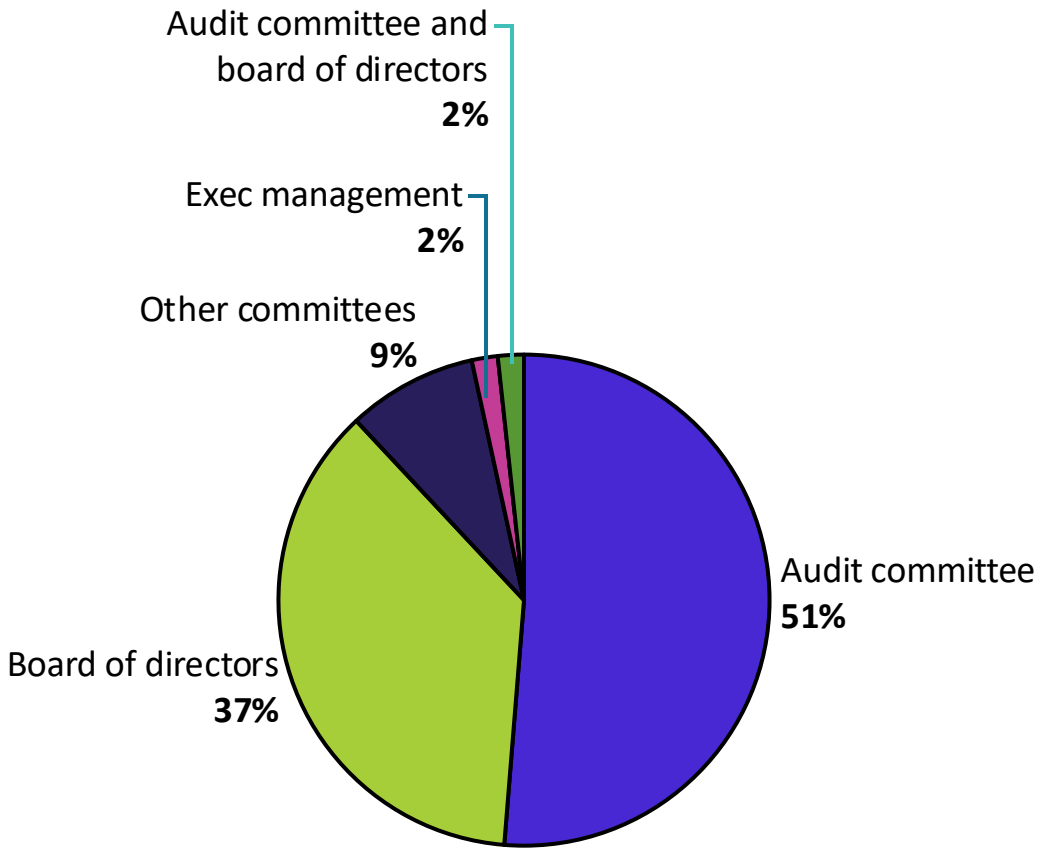
Common controls and frameworks

"Is your security organization aligned with an external framework?"

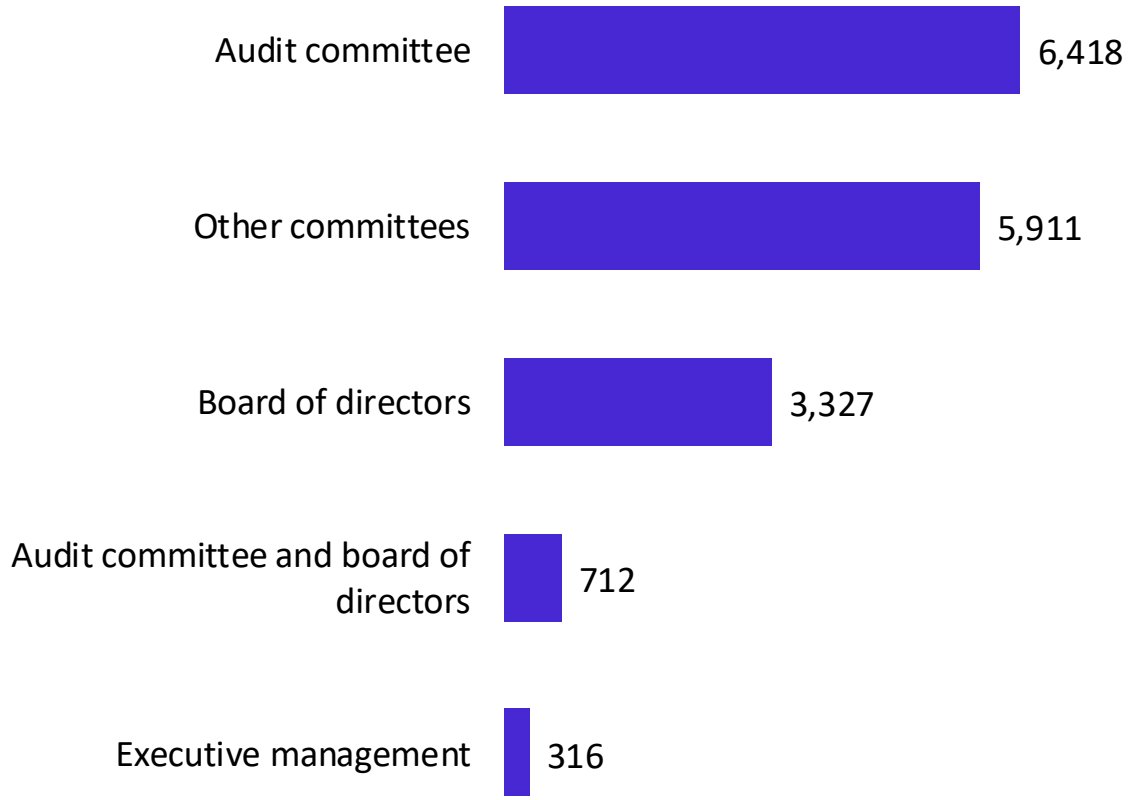


Oversight Of Cyber Risks

Oversight of cyber risks



Oversight of cyber risks by headcount



Exploiting The Definition Of Materiality

"A matter is material if there is a substantial likelihood that a reasonable investor would consider it important when determining whether to buy or sell securities."

— U.S. Securities and Exchange Commission (SEC)

Some Example Descriptions

“The audit committee is comprised entirely of independent directors, two of whom have significant work experience related to information security issues or oversight.”

— PDF Solutions

Some Example Descriptions

"A member of our audit committee and board of directors with a strong background in information technology and cybersecurity risk management through service in related senior executive positions of other publicly traded companies meets regularly with our CISO to discuss our cybersecurity risk management processes."

— Paymentus Holdings

Some Example Descriptions

"Our cybersecurity risk management and strategy processes are overseen by the cybersecurity steering committee, which includes individuals with an average of over 18 years of prior work experience in various roles involving IT governance and management, cybersecurity, auditing, and compliance."

— Monolithic Power Systems

Remember this…

"A matter is material if there is a substantial likelihood that a reasonable investor would consider it important when determining whether to buy or sell securities."

— U.S. Securities and Exchange Commission (SEC)

RSAC 2025 Conference

Other BIG Changes In 2024

Other BIG developments in 2024

- SCOTUS Chevron decision
- SCOTUS Jarkesy decision
- SEC v. SolarWinds activity
- Administration Change…

Other BIG developments in 2024

- SCOTUS Chevron decision
- SCOTUS Jarkesy decision
- SEC v. SolarWinds activity
- Administration Chang

NOTE: I AM NOT A LAWYER

Other BIG developments in 2024

- SCOTUS Chevron decision
- SCOTUS Jarkesy decision
- SEC v. SolarWinds activi
- Administration Ch

But I can predict you'll spend more on consultants and lawyers related to this this year ….

RSAC™ 2025 Conference

Here's What To Do About It

Here's What Is Keeping You Afloat…

Some Quick Takeaways

- Ambiguity is your friend for now; there are no best practices yet, **everyone** is learning
- SEC v. SolarWinds is helping quite a bit (especially in terms of **personal liability**)
- The CISO is generally not an internal director nor a signatory of these forms

What To Do Now And Next

- Tabletop / workshop your definition of materiality BEFORE an incident happens
- This is an **executive** level engagement. NOT a technical exercise.
- No technology except for email, slides, and chat software.
- If a C-level reviews log data…you have chosen poorly.

What To Do Now And Next

- Charter an information security steering committee.
- Templates exist for these committees, use a pre-existing one.
- This might already exist in your organization with a different name: Audit Committee, Cyber Steering Committee, etc.

What To Do Now And Next

- Adopt a maturity model aligned with NIST CSF
- And crosswalk it to other compliance, risk, and regulatory frameworks ASAP.
- Seriously, do the above. It will make you look amazing.

What To Do Now And Next

- Befriend internal counsel and plan to spend time with external counsel.
- Hopefully you already know these folks. If you don’t, time to meet them.

What To Do Now And Next

- Use privilege where possible – and know its limits.
- The people I just mentioned in the prior slide can help here.

What To Do Now And Next

- Work with your CFO to determine the author of your required SEC materials.
- Understand signatories, internal directors, external directors, preparers, etc.
- Are you directly authoring a section, or is the audit firm preparing your quarterly / annual materials authoring this?

RSAC™ | 2025 Conference

Many Voices.
One Community.